Introduction à la Logique Linéaire *

ROUSSEL Tristan

22 octobre 2012

Table des matières

1 Introduction **2**

2 Logique Classique **3**
2.1 Calcul des séquents 3
2.2 Élimination des coupures 4

3 Logique Linéaire **7**
3.1 Calcul des séquents 7
3.2 Élimination des coupures 9

4 Réseaux de preuves **15**
4.1 Structures de preuves 15
4.2 Critère de correction 17
4.3 Élimination des coupures 20

5 Et ensuite... **22**

*sous la direction de Claudia Faggian.

1 Introduction

Cette Introduction au Domaine de Recherche a pour but de présenter un domaine relativement récent et en plein essor : la Logique Linéaire. C'est J.-Y. Girard qui a introduit cette logique en 1987 et elle a beaucoup évoluée depuis. Depuis la découverte de la correspondance de Curry-Howard, la théorie de la démonstration est intimement liée aux systèmes de réécritures comme le λ-calcul et est à la base de résultats puissants en informatique théorique et en théorie de la calculabilité. Les notions et résultats de théorie de la démonstration sont disponibles dans les notes de cours d'O. Laurent [Lau] pour plus de précision.

2 Logique Classique

On présente d'abord la Logique Classique (LK) qui est la plus connue et utilisée en mathématiques générales.

2.1 Calcul des séquents

Définition 2.1 *On considère un ensemble $T = \{\alpha, \beta, \gamma \ldots\}$ de lettres appelées formules simples (ou types de bases) et notées par des lettre grecques minuscules. Une formule de LK est un mot défini par la grammaire suivante :*

$$A, B, C \ldots := \alpha \mid \neg A \mid A \vee B \mid A \wedge B$$

$\vee$ représente la disjonction de deux formules, $\wedge$ la conjonction de deux formules et $\neg$ la négation d'une formule. On a omis les constantes pour plus de simplicité.

Il faut maintenant définir la notion de preuve ou démonstration. On suit l'approche de G. Gentzen [Gen1, Gen2] avec le calcul des séquents.

Définitions 2.2 *Un séquent est un élement de la forme $\Gamma \vdash \Delta$ où Γ et Δ sont des multi-ensembles de formules (une formule peut être répétée un certain nombre de fois) représentés par des suites de formules séparées par des virgules. Il faut interpréter $\Gamma \vdash \Delta$ comme la conjonction des formules de Γ implique la disjonction des formules de Δ.*

Une preuve (ou démonstration) en calcul des séquents est un arbre de séquents (séparés par des barres horizontales) suivant un certain nombre de règles :

Règles structurelles

$$\frac{\Gamma_1, A, B, \Gamma_2 \vdash \Delta}{\Gamma_1, B, A, \Gamma_2 \vdash \Delta}\,\mathrm{swap}_l \qquad \frac{\Gamma \vdash \Delta_1, A, B, \Delta_2}{\Gamma \vdash \Delta_1, A, B, \Delta_2}\,\mathrm{swap}_r$$

$$\frac{\Gamma_1, A, A, \Gamma_2 \vdash \Delta}{\Gamma_1, A, \Gamma_2 \vdash \Delta}\,\mathrm{con}_l \qquad \frac{\Gamma \vdash \Delta_1, A, A, \Delta_2}{\Gamma \vdash \Delta_1, A, \Delta_2}\,\mathrm{con}_r$$

$$\frac{\Gamma_1, \Gamma_2 \vdash \Delta}{\Gamma_1, A, \Gamma_2 \vdash \Delta}\,\mathrm{weak}_l \qquad \frac{\Gamma \vdash \Delta_1, \Delta_2}{\Gamma \vdash \Delta_1, A, \Delta_2}\,\mathrm{weak}_r$$

Règles axiome et coupure

$$\frac{}{A \vdash A}\,\mathrm{ax} \qquad \frac{\Gamma_1 \vdash A, \Delta_1 \qquad \Gamma_2, A \vdash \Delta_2}{\Gamma_1, \Gamma_2 \vdash \Delta_1, \Delta_2}\,\mathrm{cut}$$

Règles $\neg$

$$\frac{\Gamma \vdash A, \Delta}{\Gamma, \neg A \vdash \Delta}\,\neg_l \qquad \frac{\Gamma, A \vdash \Delta}{\Gamma \vdash \neg A, \Delta}\,\neg_r$$

Règles $\vee$

$$\frac{\Gamma_1, A \vdash \Delta_1 \qquad \Gamma_2, B \vdash \Delta_2}{\Gamma_1, \Gamma_2, A \vee B \vdash \Delta_1, \Delta_2}\,\vee_l \qquad \frac{\Gamma \vdash A, B, \Delta}{\Gamma \vdash A \vee B, \Delta}\,\vee_r$$

Règles $\wedge$	$\dfrac{\Gamma, A, B \vdash \Delta}{\Gamma, A \wedge B \vdash \Delta}\ \wedge_l$	$\dfrac{\Gamma_1 \vdash A, \Delta_1 \qquad \Gamma_2 \vdash B, \Delta_2}{\Gamma_1, \Gamma_2 \vdash A \wedge B, \Delta_1, \Delta_2}\ \wedge_r$

On peut ne pas faire attention à l'ordre des formules grâce aux règles swap.

Exemple 2.3 *On donne ici une démonstration du tiers exclu dans LK symbolisé par la preuve suivante :*

$$\dfrac{\dfrac{\dfrac{}{A \vdash A}\ \text{ax}}{\vdash A, \neg A}\ \neg_r}{\vdash A \vee \neg A}\ \vee_r$$

2.2 Élimination des coupures

Un résultat fondamental dû à Gentzen est que la règle de coupure (assimilable à un modus ponens) est en fait inutile dans le système, elle est redondante.

Théorème 2.4 (Élimination des coupures) *Soit* Π *une preuve en calcul des séquents, il existe une preuve* Π' *de même conclusion n'utilisant pas la règle de coupure. De plus, pour rechercher une telle preuve on peut procéder à une élimination algorithmique des coupures dont on donne ici les cas principaux :*

Cas con

$$\dfrac{\dfrac{\begin{matrix}\Pi \\ \vdots \\ \Gamma_1 \vdash \Delta_1, A, A\end{matrix}}{\Gamma_1 \vdash \Delta_1, A} \qquad \begin{matrix}\Sigma \\ \vdots \\ \Gamma_2, A \vdash \Delta_2\end{matrix}}{\Gamma_1, \Gamma_2, \vdash \Delta_1, \Delta_2}$$

$$\downarrow$$

$$\dfrac{\dfrac{\dfrac{\begin{matrix}\Pi \\ \vdots \\ \Gamma_1 \vdash \Delta_1, A, A\end{matrix} \qquad \begin{matrix}\Sigma \\ \vdots \\ \Gamma_2, A \vdash \Delta_2\end{matrix}}{\Gamma_1, \Gamma_2 \vdash \Delta_1, \Delta_2, A} \qquad \begin{matrix}\Sigma \\ \vdots \\ \Gamma_2, A \vdash \Delta_2\end{matrix}}{\Gamma_1, \Gamma_2, \Gamma_2 \vdash \Delta_1, \Delta_2, \Delta_2}}{\Gamma_1, \Gamma_2 \vdash \Delta_1, \Delta_2}\ \text{con}$$

Cas weak

$$\dfrac{\dfrac{\begin{matrix}\Pi \\ \vdots \\ \Gamma_1 \vdash \Delta_1\end{matrix}}{\Gamma_1 \vdash \Delta_1, A} \qquad \begin{matrix}\Sigma \\ \vdots \\ \Gamma_2, A \vdash \Delta_2\end{matrix}}{\Gamma_1, \Gamma_2, \vdash \Delta_1, \Delta_2} \quad \rightarrow \quad \dfrac{\begin{matrix}\Pi \\ \vdots \\ \Gamma_1 \vdash \Delta_1\end{matrix}}{\Gamma_1, \Gamma_2 \vdash \Delta_1, \Delta_2}\ \text{weak}$$

Cas $\neg$

$$\dfrac{\dfrac{\begin{array}{c}\Pi\\ \vdots\\ \Gamma_1 \vdash A, \Delta_1\end{array}}{\Gamma_1, \neg A \vdash \Delta_1} \qquad \dfrac{\begin{array}{c}\Sigma\\ \vdots\\ \Gamma_2, A \vdash \Delta_2\end{array}}{\Gamma_2 \vdash \neg A, \Delta_2}}{\Gamma_1, \Gamma_2 \vdash \Delta_1, \Delta_2}$$

$$\downarrow$$

$$\dfrac{\begin{array}{c}\Pi\\ \vdots\\ \Gamma_1 \vdash A, \Delta_1\end{array} \qquad \begin{array}{c}\Sigma\\ \vdots\\ \Gamma_2, A \vdash \Delta_2\end{array}}{\Gamma_1, \Gamma_2 \vdash \Delta_1, \Delta_2}$$

Cas axiome

$$\dfrac{\begin{array}{c}\Pi\\ \vdots\\ \Gamma \vdash A, \Delta\end{array} \qquad \dfrac{}{A \vdash A}}{\Gamma \vdash A, \Delta} \quad \rightarrow \quad \begin{array}{c}\Pi\\ \vdots\\ \Gamma \vdash A, \Delta\end{array}$$

Cas $\vee_r$ - $\wedge_l$

$$\dfrac{\dfrac{\begin{array}{c}\Pi\\ \vdots\\ \Gamma \vdash \Delta, A, B\end{array}}{\Gamma \vdash \Delta, A \vee B} \qquad \dfrac{\begin{array}{c}\Sigma_1\\ \vdots\\ \Gamma_1, A \vdash \Delta_1\end{array} \quad \begin{array}{c}\Sigma_2\\ \vdots\\ \Gamma_2, B \vdash \Delta_2\end{array}}{\Gamma_1, \Gamma_2, A \wedge B \vdash \Delta_1, \Delta_2}}{\Gamma, \Gamma_1, \Gamma_2 \vdash \Delta, \Delta_1, \Delta_2}$$

$$\downarrow$$

$$\dfrac{\dfrac{\begin{array}{c}\Pi\\ \vdots\\ \Gamma \vdash \Delta, A, B\end{array} \quad \begin{array}{c}\Sigma_1\\ \vdots\\ \Gamma_1, A \vdash \Delta_1\end{array}}{\Gamma, \Gamma_1 \vdash \Delta, \Delta_1, B} \qquad \begin{array}{c}\Sigma_2\\ \vdots\\ \Gamma_2, B \vdash \Delta_2\end{array}}{\Gamma, \Gamma_1, \Gamma_2 \vdash \Delta, \Delta_1, \Delta_2}$$

$$
\dfrac{\dfrac{\begin{array}{c}\Pi\\ \vdots\\ \Gamma, A, B \vdash \Delta\end{array}}{\Gamma, A \wedge B \vdash \Delta} \quad \dfrac{\begin{array}{c}\Sigma_1\\ \vdots\\ \Gamma_1 \vdash \Delta_1, A\end{array} \quad \begin{array}{c}\Sigma_2\\ \vdots\\ \Gamma_2 \vdash \Delta_2, B\end{array}}{\Gamma_1, \Gamma_2 \vdash \Delta_1, \Delta_2, A \vee B}}{\Gamma, \Gamma_1, \Gamma_2 \vdash \Delta, \Delta_1, \Delta_2}
$$

Cas $\vee_l$ - $\wedge_r$

$$\downarrow$$

$$
\dfrac{\dfrac{\begin{array}{c}\Pi\\ \vdots\\ \Gamma, A, B \vdash \Delta\end{array} \quad \begin{array}{c}\Sigma_1\\ \vdots\\ \Gamma_1 \vdash \Delta_1, A\end{array}}{\Gamma, \Gamma_1, B \vdash \Delta, \Delta_1} \quad \begin{array}{c}\Sigma_2\\ \vdots\\ \Gamma_2 \vdash \Delta_2, B\end{array}}{\Gamma, \Gamma_1, \Gamma_2 \vdash \Delta, \Delta_1, \Delta_2}
$$

Ce résultat a des conséquences extrêmement importantes. Il permet notamment de déduire que le séquent vide $\vdash$ n'est pas prouvable, et donc que la logique classique est cohérente : on ne peut pas avoir à la fois une preuve du séquent $\vdash A$ et une preuve du séquent $\vdash \neg A$ quelle que soit la formule A. De plus, grâce à la correspondance de Curry-Howard, les étapes d'élimination des coupures peuvent être vues comme des étapes d'exécution de programmes informatiques.

Sans trop rentrer dans les détails, la correspondance de Curry-Howard établit un parallèle entre des système logiques (comme le calcul des séquents en logique classique) et les système de réécriture (comme le λ-calcul). Se correspondent formules logiques et termes, preuves et jugements de typage et enfin élimination des coupures et normalisation des termes. La programmation informatique s'appuyant en partie sur les systèmes de réécritures (comme pour le langage CAML par exemple), l'élimination des coupures prend une dimension beaucoup plus importante, et mérite d'être étudiée en tant que telle.

Malheureusement, il y a un détail très gênant en logique classique. L'élimination des coupures n'est pas confluente, c'est-à-dire qu'on peut suivre différents chemins dans l'algorithme d'élimination des coupures qui ne mènent pas à la même preuve sans coupure.

Exemple 2.5 (Paire critique de Lafont) *Supposons qu'on ait deux preuves* Π_1 *et* Π_2 *de conclusion* $\Gamma \vdash \Delta$. *Formons la preuve suivante :*

$$
\dfrac{\dfrac{\begin{array}{c}\Pi_1\\ \vdots\\ \Gamma \vdash \Delta\end{array}}{\Gamma, A \vdash \Delta} \quad \dfrac{\begin{array}{c}\Pi_2\\ \vdots\\ \Gamma \vdash \Delta\end{array}}{\Gamma \vdash A, \Delta}}{\Gamma, \Gamma \vdash \Delta, \Delta}
$$

On a deux possibilités ici pour éliminer la coupure présente. Soit on élimine l'affaiblissement à gauche, soit on élimine l'affaiblissement à droite résultant en la preuve suivante

$$\dfrac{\begin{array}{c}\Pi_i\\ \vdots\\ \Gamma \vdash \Delta\end{array}}{\Gamma, \Gamma \vdash \Delta, \Delta}$$

avec i valant 1 *ou* 2 *suivant le choix effectué. Si les preuves* Π_1 *et* Π_2 *sont différentes et sans coupure, on prouve que l'élimination des coupures n'est pas confluente.*

Le problème provient des règles structurelles qui ne sont pas contrôlées. Il existe des logiques alternatives qui permettent de contourner ce détail comme la logique intuitionniste (LJ) ou la logique linéaire (LL). La logique intuitionniste n'autorise qu'au plus une formule à droite dans un séquent et interdit l'utilisation des règles structurelles à droite, cette approche brise la symétrie du calcul. La logique linéaire inventée par J.-Y. Girard [LL] est une solution extrêmement élégante qui conserve non seulement la symétrie du calcul mais devient beaucoup plus précise et permet de penser en termes de ressources. Dans ce calcul, avoir deux fois la formule A n'est pas la même chose que de ne l'avoir qu'une seule fois.

3 Logique Linéaire

On présente ici la logique linéaire en calcul des séquents monolatère, plus simple à manipuler et parfaitement équivalente à la version bilatère.

3.1 Calcul des séquents

Définitions 3.1 *On considère un ensemble de formules simples (ou types de bases)* $T = \{\alpha, \beta, \gamma \ldots\}$ *notés par des lettres grecques minuscules. Une formule de la LL est un mot défini par la grammaire suivante :*

$$A, B, C \ldots ::= \alpha \mid \alpha^{\perp} \mid A \parr B \mid A \otimes B \mid A \,\&\, B \mid A \oplus B \mid\, !A \mid\, ?A$$

On a omis les constantes pour plus de simplicité. La formule $\alpha^{\perp}$ *est la négation linéaire de* α*, les opérateurs* $\otimes$ *et* $\&$ *sont des conjonctions, les opérateurs* $\parr$ *et* $\oplus$ *sont des disjonctions, les opérateurs* $?$ *et* $!$ *sont dits exponentiels. La formule* $!A$ *est à comprendre comme une source inépuisable de formules* A*, et* $?A$ *comme une source éventuellement vide de formules* A*.*

On définit par induction les formules de type $_^{\perp}$ *à l'aide des égalités suivantes, dites loi de De Morgan :*

$$\begin{array}{rr} (A^\perp)^\perp = A & \\ (A \parr B)^\perp = A^\perp \otimes B^\perp & (A \otimes B)^\perp = A^\perp \parr B^\perp \\ (A \,\&\, B)^\perp = A^\perp \oplus B^\perp & (A \oplus B)^\perp = A^\perp \,\&\, B^\perp \\ (!A)^\perp = ?A^\perp & (?A)^\perp = !A^\perp \end{array}$$

On utilisera la notation suivante : $A \multimap B = A^\perp \parr B$ *(par analogie avec l'implication classique* $A \to B = \neg A \vee B$*).*

Un séquent (monolatère) est un élement de la forme $\vdash \Gamma$ *où* Γ *est un multi-ensemble de formules représenté par une suite de formules séparées par des virgules. Comme en LK, il faut comprendre* $\vdash \Gamma$ *comme la preuve de la disjonction des formules de* Γ *(à partir de rien).*

Pour passer de la version bilatère du calcul à la version unilatère, on transforme le séquent $\Gamma \vdash \Delta$ *en* $\vdash \Gamma^\perp, \Delta$*.*

Une preuve est un arbre de séquents (séparés par des barres horizontales) suivant les règles de la logique linéaire :

Règles axiome et coupure	$\dfrac{}{\vdash A, A^\perp}\ \text{ax}$	$\dfrac{\vdash \Gamma, A \qquad \vdash \Delta, A^\perp}{\vdash \Gamma, \Delta}\ \text{cut}$
Règles multiplicatives	$\dfrac{\vdash \Gamma, A, B}{\vdash \Gamma, A \parr B}\ \parr$	$\dfrac{\vdash \Gamma, A \qquad \vdash \Delta, B}{\vdash \Gamma, \Delta, A \otimes B}\ \otimes$
Règles additives	$\dfrac{\vdash \Gamma, A}{\vdash \Gamma, A \oplus B}\ \oplus_1$ $\dfrac{\vdash \Gamma, B}{\vdash \Gamma, A \oplus B}\ \oplus_2$	$\dfrac{\vdash \Gamma, A \qquad \vdash \Gamma, B}{\vdash \Gamma, A \,\&\, B}\ \&$
Règles exponentielles	$\dfrac{\vdash \Gamma, A}{\vdash \Gamma, ?A}\ ?_{\text{der}}$ $\dfrac{\vdash \Gamma}{\vdash \Gamma, ?A}\ ?_{\text{weak}}$	$\dfrac{\vdash ?\Gamma, A}{\vdash ?\Gamma, !A}\ !$ $\dfrac{\vdash \Gamma, ?A, ?A}{\vdash \Gamma, ?A}\ ?_{\text{con}}$

Une preuve d'une formule A *est simplement une preuve d'unique conclusion* A *sans prémisse.*

Les règles exponentielles servent à contrôler les règles structurelles d'affaiblissement et de contraction et permettent d'obtenir une élimination des coupures confluente.

3.2 Élimination des coupures

Un résultat crucial concernant la logique linéaire est le théorème d'élimination des coupures, et la procédure d'élimination qui en découle. Le calcul des séquents introduit originellement par G. Gentzen pour la logique classique (et intuitionniste) permet grâce à la propriété de la sous-formule d'avoir une procédure automatique de recherche de preuves (avec quelques restrictions) sans coupure.

Théorème 3.2 (Élimination des coupures) *Soit* Π *une preuve en calcul des séquents, il existe une preuve* Π' *de même conclusion n'utilisant pas la règle de coupure. De plus, pour rechercher une telle preuve on peut procéder à une élimination algorithmique des coupures dont on donne ici les cas principaux :*

Cas axiome

$$\dfrac{\begin{array}{c}\Pi\\ \vdots\\ \vdash \Gamma, A\end{array} \qquad \dfrac{}{\vdash A, A^{\perp}}}{\vdash \Gamma, A} \quad \rightarrow \quad \begin{array}{c}\Pi\\ \vdots\\ \vdash \Gamma, A\end{array}$$

Cas $\parr$ - $\otimes$

$$\dfrac{\dfrac{\begin{array}{c}\Pi\\ \vdots\\ \vdash \Gamma, A, B\end{array}}{\vdash \Gamma, A \parr B} \qquad \dfrac{\begin{array}{c}\Sigma_1\\ \vdots\\ \vdash \Delta_1, A^{\perp}\end{array} \qquad \begin{array}{c}\Sigma_2\\ \vdots\\ \vdash \Delta_2, B^{\perp}\end{array}}{\vdash \Delta_1, \Delta_2, A^{\perp} \otimes B^{\perp}}}{\vdash \Gamma, \Delta_1, \Delta_2}$$

$$\downarrow$$

$$\dfrac{\dfrac{\begin{array}{c}\Pi\\ \vdots\\ \vdash \Gamma, A, B\end{array} \qquad \begin{array}{c}\Sigma_1\\ \vdots\\ \vdash \Delta_1, A^{\perp}\end{array}}{\vdash \Gamma, \Delta_1, B} \qquad \begin{array}{c}\Sigma_2\\ \vdots\\ \vdash \Delta_2, B^{\perp}\end{array}}{\vdash \Gamma, \Delta_1, \Delta_2}$$

Cas $\oplus_i$ - &

$$\dfrac{\dfrac{\begin{array}{c}\Pi\\ \vdots\\ \vdash \Gamma, A_i\end{array}}{\vdash \Gamma, A_1 \oplus A_2} \qquad \dfrac{\begin{array}{c}\Sigma_1\\ \vdots\\ \vdash \Delta, A_1^\perp\end{array} \quad \begin{array}{c}\Sigma_2\\ \vdots\\ \vdash \Delta, A_2^\perp\end{array}}{\vdash \Delta, A_1^\perp \,\&\, A_2^\perp}}{\vdash \Gamma, \Delta}$$

$$\downarrow$$

$$\dfrac{\begin{array}{c}\Pi\\ \vdots\\ \vdash \Gamma, A_i\end{array} \qquad \begin{array}{c}\Sigma_i\\ \vdots\\ \vdash \Delta, A_i^\perp\end{array}}{\vdash \Gamma, \Delta}$$

Cas $?_{\text{der}}$ - !

$$\dfrac{\dfrac{\begin{array}{c}\Pi\\ \vdots\\ \vdash \Gamma, A\end{array}}{\vdash \Gamma, ?A} \qquad \dfrac{\begin{array}{c}\Sigma\\ \vdots\\ \vdash ?\Delta, A^\perp\end{array}}{\vdash ?\Delta, !A^\perp}}{\vdash \Gamma, ?\Delta} \quad \rightarrow \quad \dfrac{\begin{array}{c}\Pi\\ \vdots\\ \vdash \Gamma, A\end{array} \qquad \begin{array}{c}\Sigma\\ \vdots\\ \vdash ?\Delta, A^\perp\end{array}}{\vdash \Gamma, ?\Delta}$$

Cas $?_{\text{weak}}$ - !

$$\dfrac{\dfrac{\begin{array}{c}\Pi\\ \vdots\\ \vdash \Gamma\end{array}}{\vdash \Gamma, ?A} \qquad \dfrac{\begin{array}{c}\Sigma\\ \vdots\\ \vdash ?\Delta, A^\perp\end{array}}{\vdash ?\Delta, !A^\perp}}{\vdash \Gamma, ?\Delta} \quad \rightarrow \quad \begin{array}{c}\Pi\\ \vdots\\ \vdash \Gamma\\ = = = = = \ ?_{weak}\\ \vdash \Gamma, ?\Delta\end{array}$$

Cas $?_{\text{con}}$ - !

$$\dfrac{\dfrac{\begin{array}{c}\Pi\\ \vdots\\ \vdash \Gamma, ?A, ?A\end{array}}{\vdash \Gamma, ?A} \qquad \dfrac{\begin{array}{c}\Sigma\\ \vdots\\ \vdash ?\Delta, A^\perp\end{array}}{\vdash ?\Delta, !A^\perp}}{\vdash \Gamma, ?\Delta}$$

$$\downarrow$$

$$\begin{array}{c}\dfrac{\dfrac{\begin{array}{c}\Pi\\ \vdots\\ \vdash \Gamma, ?A, ?A\end{array} \qquad \begin{array}{c}\Sigma\\ \vdots\\ \vdash ?\Delta, A^\perp\end{array}}{\vdash \Gamma, ?\Delta, ?A} \qquad \begin{array}{c}\Sigma\\ \vdots\\ \vdash ?\Delta, A^\perp\end{array}}{\vdash \Gamma, ?\Delta, ?\Delta}\\ = = = = = = = \ ?_{con}\\ \vdash \Gamma, ?\Delta\end{array}$$

Les doubles barres discontinues signifient que la règle est utilisée plusieurs fois.

Il existe aussi un certain nombre de règles de commutation qui correspondent aux cas où la formule coupée n'est pas directement introduite par les deux séquents coupés. À chaque fois, on fait remonter la coupure dans la preuve pour se rapprocher de l'introduction de la formule coupée. On présente ici les commutations pour les formules de droites, elles sont analogues pour les formules de gauche.

Commutation ⊗ 1

$$\dfrac{\begin{matrix}\Pi\\ \vdots\\ \vdash \Gamma, C\end{matrix} \qquad \dfrac{\begin{matrix}\Sigma_1\\ \vdots\\ \vdash \Delta_1, A, C^\perp\end{matrix} \qquad \begin{matrix}\Sigma_2\\ \vdots\\ \vdash \Delta_2, B\end{matrix}}{\vdash \Delta_1, \Delta_2, A \otimes B, C^\perp}}{\vdash \Gamma, \Delta_1, \Delta_2, A \otimes B}$$

$$\downarrow$$

$$\dfrac{\dfrac{\begin{matrix}\Pi\\ \vdots\\ \vdash \Gamma, C\end{matrix} \qquad \begin{matrix}\Sigma_1\\ \vdots\\ \vdash \Delta_1, A, C^\perp\end{matrix}}{\vdash \Gamma, \Delta_1, A} \qquad \begin{matrix}\Sigma_2\\ \vdots\\ \vdash \Delta_2, B\end{matrix}}{\vdash \Gamma, \Delta_1, \Delta_2, A \otimes B}$$

Commutation ⊗ 2

$$\dfrac{\begin{matrix}\Pi\\ \vdots\\ \vdash \Gamma, C\end{matrix} \qquad \dfrac{\begin{matrix}\Sigma_1\\ \vdots\\ \vdash \Delta_1, A\end{matrix} \qquad \begin{matrix}\Sigma_2\\ \vdots\\ \vdash \Delta_2, B, C^\perp\end{matrix}}{\vdash \Delta_1, \Delta_2, A \otimes B, C^\perp}}{\vdash \Gamma, \Delta_1, \Delta_2, A \otimes B}$$

$$\downarrow$$

$$\dfrac{\begin{matrix}\Sigma_1\\ \vdots\\ \vdash \Delta_1, A\end{matrix} \qquad \dfrac{\begin{matrix}\Pi\\ \vdots\\ \vdash \Gamma, C\end{matrix} \qquad \begin{matrix}\Sigma_2\\ \vdots\\ \vdash \Delta_2, B, C^\perp\end{matrix}}{\vdash \Gamma, \Delta_2, B}}{\vdash \Gamma, \Delta_1, \Delta_2, A \otimes B}$$

Commutation $\parr$

$$\dfrac{\begin{matrix}\Pi\\ \vdots\\ \vdash \Gamma, C\end{matrix} \qquad \dfrac{\begin{matrix}\Sigma\\ \vdots\\ \vdash \Delta, A, B, C^\perp\end{matrix}}{\vdash \Delta, A \parr B, C^\perp}}{\vdash \Gamma, \Delta, A \parr B}$$

$$\downarrow$$

$$\dfrac{\dfrac{\begin{matrix}\Pi\\ \vdots\\ \vdash \Gamma, C\end{matrix} \qquad \begin{matrix}\Sigma\\ \vdots\\ \vdash \Delta, A, B, C^\perp\end{matrix}}{\vdash \Gamma, \Delta, A, B}}{\vdash \Gamma, \Delta, A \parr B}$$

Commutation $\&$

$$\dfrac{\begin{matrix}\Pi\\ \vdots\\ \vdash \Gamma, C\end{matrix} \qquad \dfrac{\begin{matrix}\Sigma_1\\ \vdots\\ \vdash \Delta, A, C^\perp\end{matrix} \qquad \begin{matrix}\Sigma_2\\ \vdots\\ \vdash \Delta, B, C^\perp\end{matrix}}{\vdash \Delta, A \,\&\, B, C^\perp}}{\vdash \Gamma, \Delta, A \,\&\, B}$$

$$\downarrow$$

$$\dfrac{\dfrac{\begin{matrix}\Pi\\ \vdots\\ \vdash \Gamma, C\end{matrix} \qquad \begin{matrix}\Sigma_1\\ \vdots\\ \vdash \Delta, A, C^\perp\end{matrix}}{\vdash \Gamma, \Delta, A} \qquad \dfrac{\begin{matrix}\Pi\\ \vdots\\ \vdash \Gamma, C\end{matrix} \qquad \begin{matrix}\Sigma_2\\ \vdots\\ \vdash \Delta, B, C^\perp\end{matrix}}{\vdash \Gamma, \Delta, B}}{\vdash \Gamma, \Delta, A \,\&\, B}$$

Commutation $\oplus_i$

$$\dfrac{\begin{matrix}\Pi\\ \vdots\\ \vdash \Gamma, C\end{matrix} \qquad \dfrac{\begin{matrix}\Sigma\\ \vdots\\ \vdash \Delta, A_i, C^\perp\end{matrix}}{\vdash \Delta, A_1 \oplus A_2, C^\perp}}{\vdash \Gamma, \Delta, A_1 \oplus A_2}$$

$$\downarrow$$

$$\dfrac{\dfrac{\begin{matrix}\Pi\\ \vdots\\ \vdash \Gamma, C\end{matrix} \qquad \begin{matrix}\Sigma\\ \vdots\\ \vdash \Delta, A_i, C^\perp\end{matrix}}{\vdash \Gamma, \Delta, A_i}}{\vdash \Gamma, \Delta, A_1 \oplus A_2}$$

Commutation $?_{\text{der}}$

$$\dfrac{\begin{matrix}\Pi\\ \vdots\\ \vdash \Gamma, C\end{matrix} \qquad \dfrac{\begin{matrix}\Sigma\\ \vdots\\ \vdash \Delta, A, C^{\perp}\end{matrix}}{\vdash \Delta, ?A, C^{\perp}}}{\vdash \Gamma, \Delta, ?A}$$

$$\downarrow$$

$$\dfrac{\dfrac{\begin{matrix}\Pi\\ \vdots\\ \vdash \Gamma, C\end{matrix} \qquad \begin{matrix}\Sigma\\ \vdots\\ \vdash \Delta, A, C^{\perp}\end{matrix}}{\vdash \Gamma, \Delta, A}}{\vdash \Gamma, \Delta, ?A}$$

Commutation $?_{\text{weak}}$

$$\dfrac{\begin{matrix}\Pi\\ \vdots\\ \vdash \Gamma, C\end{matrix} \qquad \dfrac{\begin{matrix}\Sigma\\ \vdots\\ \vdash \Delta, C^{\perp}\end{matrix}}{\vdash \Delta, ?A, C^{\perp}}}{\vdash \Gamma, \Delta, ?A}$$

$$\downarrow$$

$$\dfrac{\dfrac{\begin{matrix}\Pi\\ \vdots\\ \vdash \Gamma, C\end{matrix} \qquad \begin{matrix}\Sigma\\ \vdots\\ \vdash \Delta, C^{\perp}\end{matrix}}{\vdash \Gamma, \Delta}}{\vdash \Gamma, \Delta, ?A}$$

Commutation $?_{\text{con}}$

$$\dfrac{\begin{matrix}\Pi\\ \vdots\\ \vdash \Gamma, C\end{matrix} \qquad \dfrac{\begin{matrix}\Sigma\\ \vdots\\ \vdash \Delta, ?A, ?A, C^{\perp}\end{matrix}}{\vdash \Delta, ?A, C^{\perp}}}{\vdash \Gamma, \Delta, ?A}$$

$$\downarrow$$

$$\dfrac{\dfrac{\begin{matrix}\Pi\\ \vdots\\ \vdash \Gamma, C\end{matrix} \qquad \begin{matrix}\Sigma\\ \vdots\\ \vdash \Delta, ?A, ?A, C^{\perp}\end{matrix}}{\vdash \Gamma, \Delta, ?A, ?A}}{\vdash \Gamma, \Delta, ?A}$$

Commutation !

$$\dfrac{\begin{array}{c}\Pi\\ \vdots\\ \vdash ?\Gamma, !C\end{array} \quad \dfrac{\begin{array}{c}\Sigma\\ \vdots\\ \vdash ?\Delta, A, ?C^\perp\end{array}}{\vdash ?\Delta, !A, ?C^\perp}}{\vdash ?\Gamma, ?\Delta, !A}$$

$$\downarrow$$

$$\dfrac{\dfrac{\begin{array}{c}\Pi\\ \vdots\\ \vdash ?\Gamma, !C\end{array} \quad \begin{array}{c}\Sigma\\ \vdots\\ \vdash ?\Delta, A, ?C^\perp\end{array}}{\vdash ?\Gamma, ?\Delta, A}}{\vdash ?\Gamma, ?\Delta, !A}$$

PREUVE DU THÉORÈME. La première étape est de vérifier qu'on couvre bien tous les cas avec nos étapes d'élimination des coupures et de commutation. Il pourrait y avoir un problème dans le dernier cas de commutation si la conclusion de Π n'était pas de la forme $\vdash ?\Gamma, !C$. Une récurrence simple prouve que toute preuve qui a une formule de la forme $!A$ dans sa conclusion a toutes les autres formules de sa conclusion de la forme $?B$. Tant qu'il reste une coupure dans la preuve, on peut appliquer une étape.

La preuve classique de l'élimination des coupures s'appuie sur les candidats de réductibilité. Néanmoins, celle-ci est assez peu visuelle, étant une preuve sémantique. On prouve ici l'élimination pour la classe des preuves ne contenant pas de contraction pour mieux faire comprendre ce qu'il se passe. On voit notamment que la propriété de sous-formule du calcul des séquents (les formules introduites sont toujours plus complexes que les formules dont elles proviennent) a un intérêt majeur dans la démonstration.

On définit le rang d'une coupure comme la somme des distances dans l'arbre de preuve entre la coupure et les règle d'introduction des deux formules coupées. Les cas principaux correspondent au rang minimal 2 d'une formule et soit détruisent la coupure, soit la remplacent par des coupures sur des formules moins complexes. Les cas de commutation font diminuer le rang des coupures.

On raisonne par induction sur la liste $(c_i, r_i)_{i\in I}$ où I est la liste des coupures rangées par ordre décroissant de complexité (de formules coupées), c_i est la complexité des formules coupées de la coupure i et r_i et le rang de la coupure i. On munit cette liste de l'ordre lexicographique (les couples à l'intérieur sont aussi munis de cet ordre). On agit d'abord sur les coupures les plus complexes en premier, et on fait d'abord les cas principaux si possibles. Dans un cas principal, on ajoute éventuellement des coupures mais on réduit la plus grande complexité (ou on supprime complètement la coupure), donc la liste $(c_i, r_i)_{i\in I}$ diminue. Dans un cas de commutation, on ajoute éventuellement des coupures mais on réduit le rang de la coupure la plus complexe sans en ajouter de plus complexes strictement, donc la liste diminue tout autant. L'ordre défini est

bien fondé, donc par induction l'algorithme termine.

Pour la confluence, c'est un peu fastidieux de couvrir tous les cas. On donne juste l'idée de la démonstration. Si on a deux éliminations de coupures possibles dans une preuve, deux cas peuvent se présenter : soit elles sont indépendantes en le sens qu'on peut effectuer l'une puis « l'autre » (plus exactement le résidu de l'autre coupure) ou l'autre puis « l'une » (toujours le résidu), soit on a deux coupures imbriquées l'une dans l'autre, à savoir qu'on est dans l'un des deux cas suivants :

$$\begin{array}{c}\dfrac{\vdash A, A^\perp \qquad \vdash A, A^\perp}{\vdash A, A^\perp} \\ \vdots\end{array} \qquad\qquad \dfrac{\dfrac{\begin{array}{c}\vdots\\ \vdash \Gamma, A\end{array} \qquad \vdash A, A^\perp}{\vdash \Gamma, A} \qquad \begin{array}{c}\vdots\\ \vdash \Delta, A^\perp\end{array}}{\vdash \Gamma, \Delta}$$

On peut en fait vérifier que dans chacun des cas, éliminer l'une ou l'autre des coupures produit exactement le même résultat in fine.

□

L'élimination des coupures est assez fastidieuse en pratique et on a l'impression que les phases de commutation ne sont pas des étapes essentielles du calcul, ce qui nous pousse à essayer d'adopter un modèle plus visuel des preuves. On est pour cela obligé de réduire notre champ de preuves en oubliant les opérateurs additifs qui s'adaptent mal à la suite.

4 Réseaux de preuves

On considère le fragment MELL (Multiplicative Exponential Linear Logic) de la logique linéaire qui ne contient plus les opérateurs & et $\oplus$ ni les règles associées à ces opérateurs. La notion de réseau de preuve est beaucoup plus géométrique et moins lourde que le calcul des séquents.

4.1 Structures de preuves

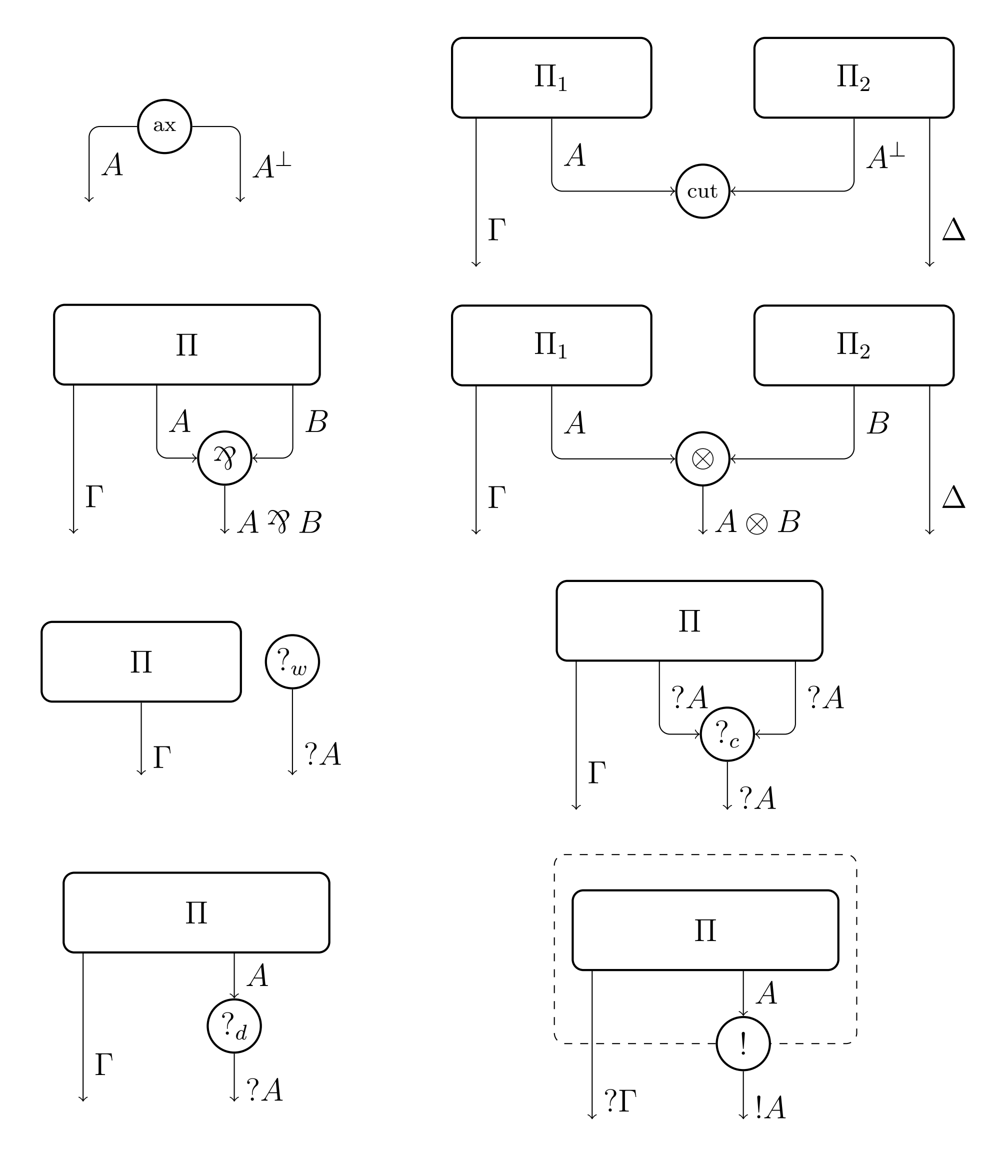
Définition 4.1 *On appelle* **structure de preuve** *un graphe orienté dont les sommets (appelés aussi nœuds) sont étiquetés soit par des opérateurs de la logique linéaire (⅋, $\otimes$, ! et ?) soit par* **ax** *(pour axiome) ou* **cut** *(pour coupure) et les arêtes sont étiquetées par des formules de la logique linéaire en respectant certaines règles. Le graphe a aussi des arêtes pendantes (arêtes sortantes qui ne rentrent pas dans un nœud) qui correspondent aux conclusions de la structure de preuve.*

Les nœuds ont autant d'arêtes entrantes (appelées prémisses) que leurs opérateurs liés ont de séquents nécessaires à leur introduction dans leur règles associées et ils ont chacun une arête sortante (appelée conclusion). Pour **ax**

le nœud a deux conclusions et pas de prémisse, et pour **cut** *le nœud a deux prémisses et pas de conclusion.*

Le nœud ! est un peu particulier. Il vient avec une « boîte », telle que toutes les arêtes sortantes de la boîte à par la conclusion du ! soient de types qui commencent par ?, et qu'il n'y ait pas d'arête entrante dans la boîte. Dans une structure de preuve, deux boîtes, sont soit incluses l'une dans l'autre soit disjointes.

Cette définition se comprend mieux en considérant la construction inductive des structures de preuve. Les structures de preuves sont construites de la manière suivante :



où Π*,* Π_1 *et* Π_2 *représentent des structures de preuves. Les liens étiquetés par des multi-ensembles (*Γ*,* Δ *et* $?\Gamma$*) sont en fait un ensemble de liens, chacun étiqueté par un élément du multi-ensemble. Les nœuds* **ax** *et* **cut** *seront souvent omis par souci d'économie, de même les étiquetages des liens seront parfois*

succints. Le nœud $?_w$ vient aussi avec un «jump» vers un autre nœud, qui est un lien qui ne sert que pour le critère de correction.

La raison pour laquelle on choisit d'avoir une ou deux structures de preuves en prémisse d'une règle provient du critère de correction des réseaux de preuves présenté plus loin.

Remarques 4.2 *La boîte du nœud ! sert à vérifier si le contexte de la structure de preuve au moment de l'introduction de ce nœud est bien de la forme $?\Gamma$. Elle permet de contrôler la commutation des règles dans le contexte entre avant et après elle. C'est le seul cas où on conserve cette commutation.*

Définition 4.3 *On définit par induction sur la dernière règle utilisée la traduction d'une preuve en calcul des séquents de* **MELL** *en structure de preuve. Cette définition est complètement naturelle.*

On appelle **réseau de preuve** *toute structure de preuve qui est l'image d'une preuve en calcul des séquents par cette transformation.*

4.2 Critère de correction

Il existe un critère assez simple qui permet de savoir si une structure de preuve est un réseau de preuve. Un premier critère a été introduit par J.-Y. Girard (critère du long voyage) [LL], puis un autre équivalent et un peu plus simple a été dévouvert par V. Danos et L. Regnier [Cor].

Définitions 4.4 *On appelle* **switching** *(ou interrupteur) d'une structure de preuve les choix pour chaque nœud $\parr$ d'une des deux prémisses. On appelle* **graphe de correction** *associé à une structure de preuve et un switching le graphe non-orienté défini par :*

- *les sommets sont les nœuds et boîtes (on écrase le contenu d'une boîte en un seul nœud) de la structure de preuve (on rajoute un nœud par conclusion de la structure de preuve),*
- *les arêtes sont les liens entre les nœuds de la structure de preuve (tous les liens sortant d'une boîte deviennent des arêtes partant du sommet associé),*
- *toutes les prémisses des nœuds $\parr$ sont effacées,*
- *les liens choisis par le switching sont rajoutés.*
- *les jumps sont rajoutés comme vrais liens.*

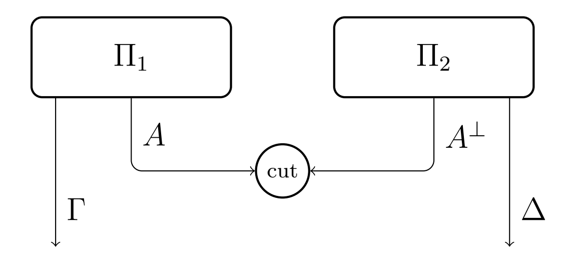
Théorème 4.5 (critère de correction de Danos-Regnier) *Une structure de preuve sans boîte est un réseau de preuve si et seulement si tous ses graphes de correction (associés à tous ses switchings) sont connexes et acycliques.*

Une strucutre de preuve avec boîte est un réseau de preuve si et seulement si les sous-structures incluses dans les boîtes sont des réseaux de preuves et tous ses graphes de correction sont connexes et acycliques.

Preuve du Théorème. La preuve se fait en deux temps. On ne prouvera que la partie facile, qui est qu'un réseau de preuve vérifie le critère de correction. Pour l'autre partie, la preuve classique utilise les empires introduits par J.-Y. Girard, cependant une approche récente de P. Di Giamberardino et de C. Faggian [Seq] permet sûrement de simplifier la preuve.

La traduction d'une preuve ne contenant qu'un axiome vérifie bien le critère de correction. Il s'agit simplement d'un nœud axiome à deux conclusions. Il n'y a donc qu'un switching possible et le graphe de correction associé est connexe et acyclique.

On raisonne par récurrence, on suppose que l'on a prouvé que tout réseau de preuve à moins de n nœuds vérifie le critère de correction. Soit un réseau de preuve à $n + 1$ nœuds. Considérons le dernier nœud de sa construction inductive. S'il s'agit d'un nœud coupure, alors il existe deux preuves Π_1 et Π_2 telles que le réseau soit :



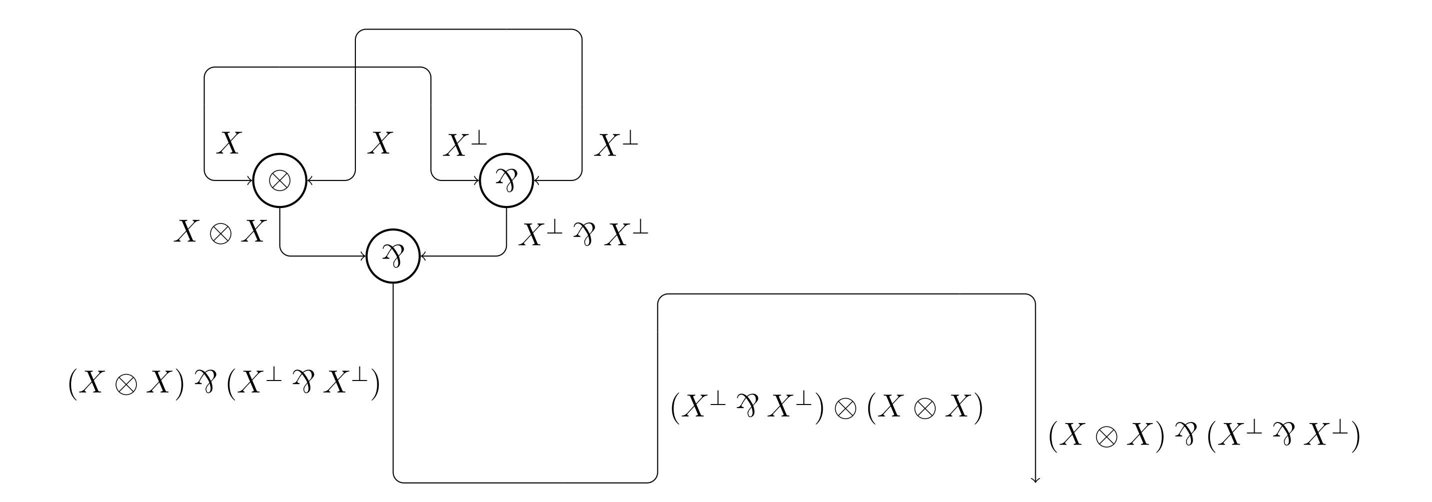
Par récurrence, les réseaux Π_1 et Π_2 sont corrects. Soit un switching σ du réseau de preuve, il existe deux switchings σ_1 et σ_2 tels que $\sigma = \sigma_1 \cup \sigma_2$. Par correction de Π_1 et Π_2 les graphes de correction associés à σ_1 et σ_2 sont connexes et acycliques, comme le graphe de correction associé à σ est simplement l'union des deux graphes de correction associés à σ_1 et σ_2 avec un lien entre les deux, il est aussi connexe et acyclique.

Tous les nœuds sans boîte se traitent de manière similaire. Le nœud ! est assez simple aussi, son réseau à l'intérieur est correct par récurrence, et le réseau avec boîte vérifie bien le critère de correction.

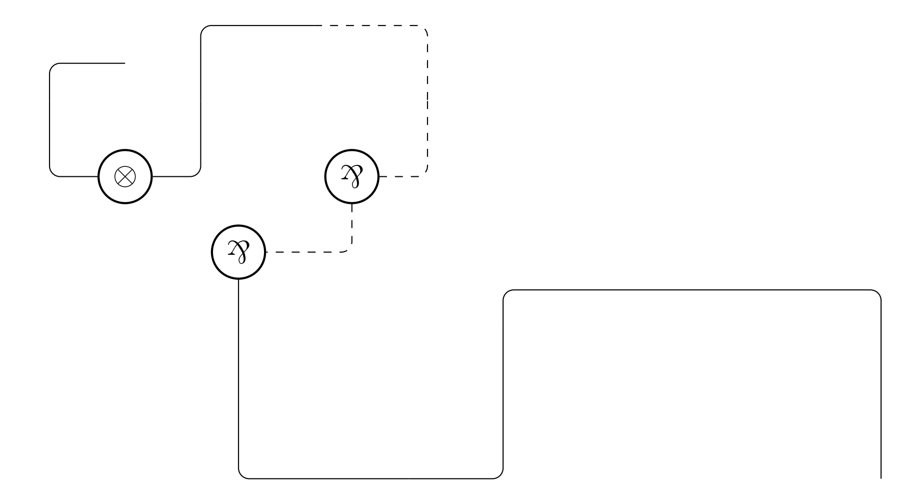
Donc, par récurrence, tous les réseaux de preuves vérifient le critère de correction.

□

Exemple 4.6 *Considérons la structure de preuve suivante :*



On veut savoir si c'est un réseau de preuve. Il y a 4 switchings possibles : il y a deux choix par nœud $\parr$*. On peut vérifier facilement que tous ses graphes des correction sont bien connexes acycliques, en voici un exemple :*



Les arêtes discontinues correspondent aux liens choisis par le switching. On peut vérifier que cette structure de preuve provient de la preuve suivante en calcul des séquents :

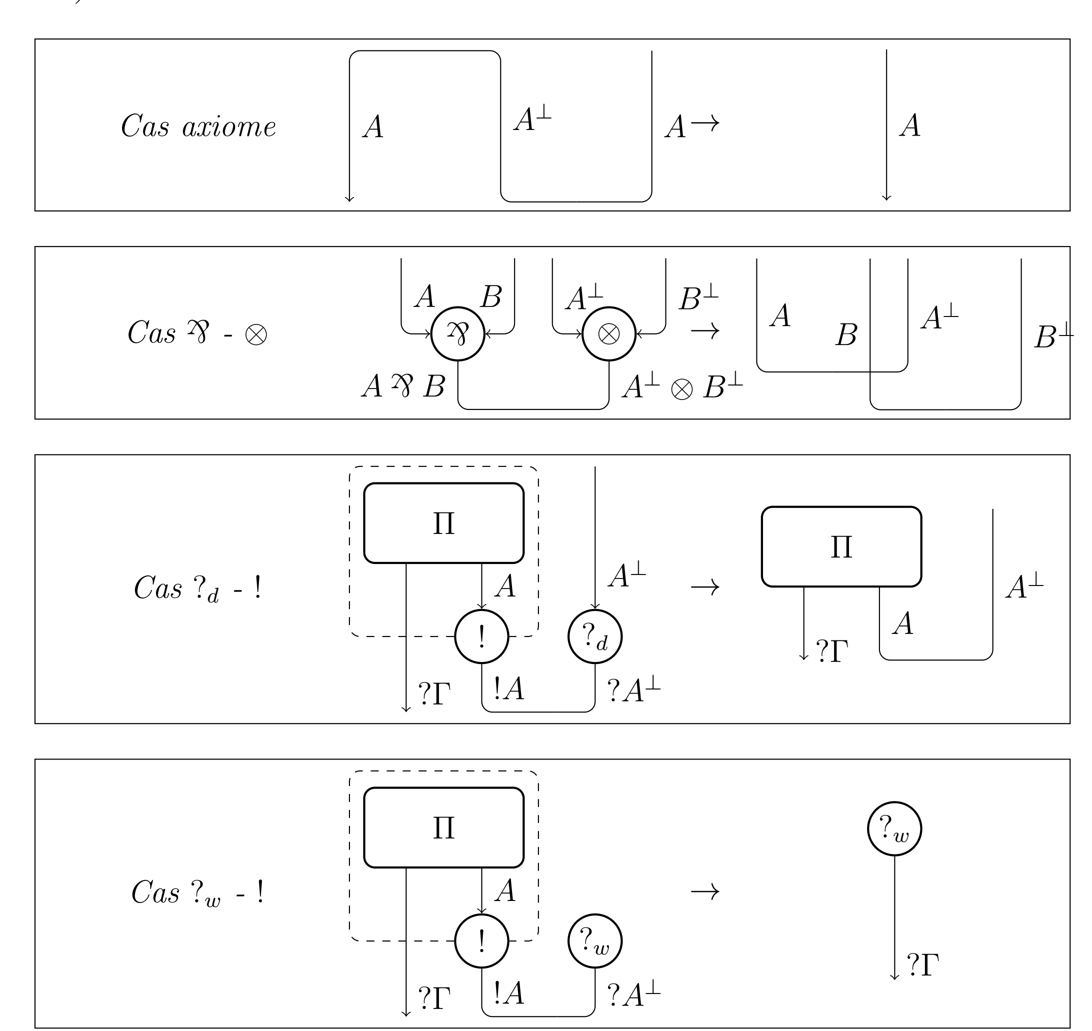
$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\vdash X, X^\perp} \quad \dfrac{}{\vdash X, X^\perp}}{\vdash X \otimes X, X^\perp, X^\perp}}{\vdash X \otimes X, X^\perp \parr X^\perp}}{\vdash (X \otimes X) \parr (X^\perp \parr X^\perp)} \qquad \dfrac{}{\vdash (X^\perp \parr X^\perp) \otimes (X \otimes X), (X \otimes X) \parr (X^\perp \parr X^\perp)}}{\vdash (X \otimes X) \parr (X^\perp \parr X^\perp)}$$

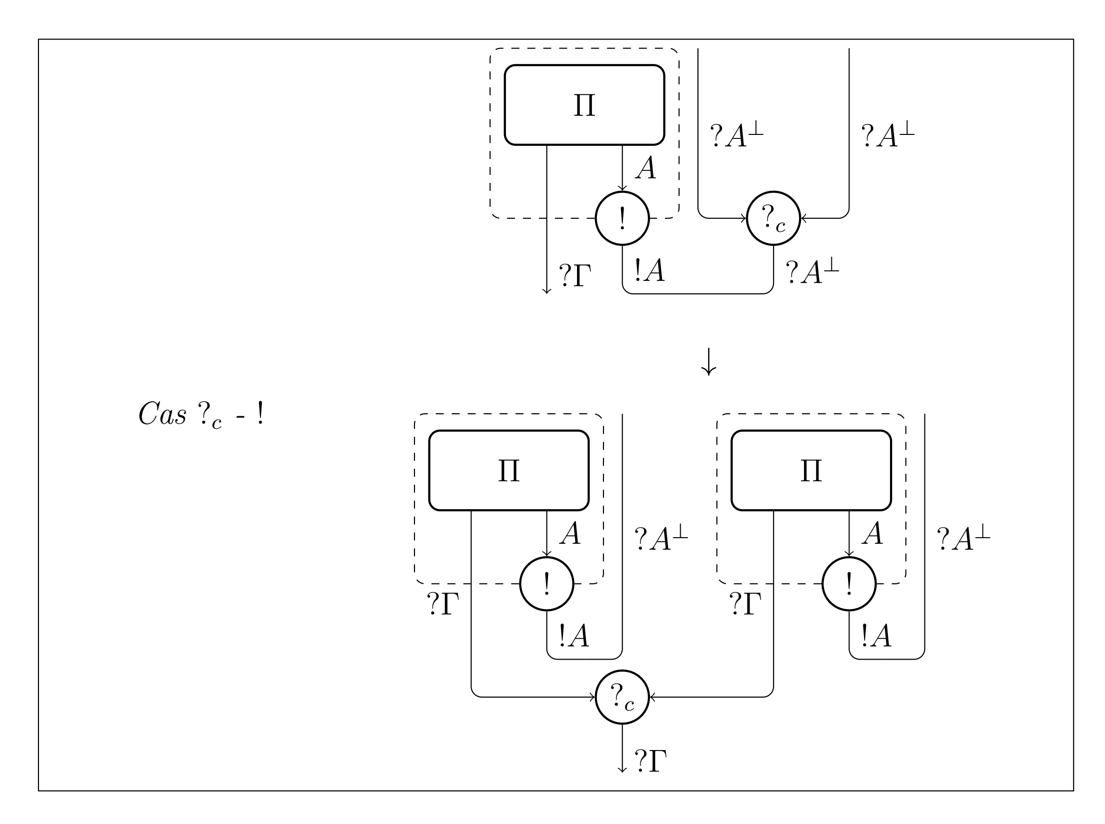
La preuve du critère de correction se fait par la ***séquentialisation*** des réseaux de preuves, c'est-à-dire la transformation des réseaux de preuves en preuves du calcul des séquents.

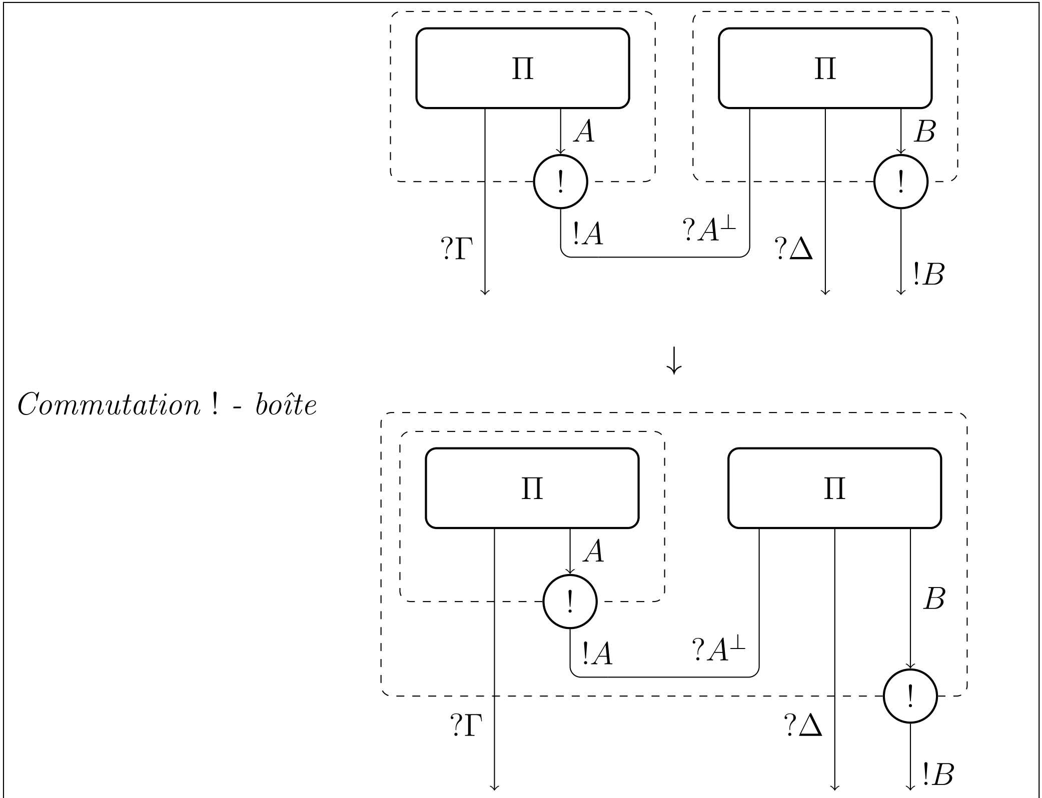
4.3 Élimination des coupures

On s'intéresse maintenant à la procédure d'élimination des coupures : comment se traduit-elle dans les réseaux de preuves ?

Proposition 4.7 *L'élimination des coupures dans les réseaux de preuves se traduit par les règles locales suivantes (applicables à toutes les structures de preuve) :*







Plus précisément, appliquer l'élimination des coupures à une preuve en calcul des séquents puis la traduire en réseau de preuve revient au même que de traduire d'abord la preuve en réseau de preuve puis d'appliquer les étapes d'élimination des coupures des structures de preuve.

On a aussi que l'élimination des coupures dans les structures de preuves conserve le critère de correction.

5 Et ensuite...

L'étape suivante serait de présenter la Géométrie de l'Interaction introduite par J.-Y. Girard qui est à la base de la sémantique des jeux et qui est un outil extrêmement puissant en théorie de la démonstration. C'est une sémantique de la logique linéaire opérationnelle (permettant de calculer pas à pas l'élimination des coupures sur les réseaux de preuve aussi bien que sur le calcul des séquents) très géométrique et intuitive. Elle est notamment à la base de la sémantique des jeux et de la ludique.

Références

[Gen1] G. Gentzen (1935) *Untersuchungen über das logische Schließen. I*, Mathematische Zeitschrift, Volume 39

[Gen2] G. Gentzen (1935) *Untersuchungen über das logische Schließen. II*, Mathematische Zeitschrift, Volume 39

[PnT] J.-Y. Girard, Y. Lafont et P. Taylor (1989) *Proofs and Types*, Cambridge University Press

[LL] J.-Y. Girard (1987) *Linear Logic*, Theoretical Computer Science, Volume 50

[Lau] O. Laurent (2008), *Théorie de la démonstration*, notes de cours, disponible sur Internet : `http://perso.ens-lyon.fr/olivier.laurent/thdem.pdf`

[Cor] V. Danos et L. Regnier (1989), *The structure of multiplicatives*, Archive for Mathematical Logic Volume 28, p. 181-203

[Seq] P. Di Giamberardino et C. Faggian (2006), *Jump from Parallel to Sequential Proofs : Multiplicatives*, Computer Science Logic Volume 6, Springer